# Optimization of Security in Hybrid Networks using Computational Intelligence

**SHORT SYNOPSIS**

*Submitted in partial fulfillment of the requirement of the degree of*

## DOCTOR OF PHILOSOPHY

*to*

*Manav Rachna International Institute of Research and Studies*
*(Deemed to be University)*

*by*

**Ashu**
Registration number: 17/PhD/038

Under the supervision of
**Dr.Rashima Mahajan**
**Associate Professor, Faculty of Engineering and Technology, MRIIRS**

Joint Supervisor
**Dr.Sherin Zafar**
**Assistant Professor, Department of CSE, SEST, Jamia Hamdard, New Delhi**

FACULTY OF ENGINEERING & TECHNOLOGY

MANAV RACHNA INTERNATIONAL INSTITUTE OF RESEARCH & STUDIES

SECTOR-43, SURAJKUND –DELHI ROAD, FARIDABAD – 121001

## FACULTY OF ENGINEERING & TECHNOLOGY

## Certificate

I hereby declare that the short synopsis “Optimization of Security in Hybrid Networks using Computational Intelligence" being submitted in partial fulfillment of the requirement for the degree of Doctor of Philosophy in Electronics and Communication under Faculty of Engineering and Technology, Manav Rachna International Institute of Research & Studies, Faridabad during the academic year 2018-2019.

It is a bonafide record of original work carried out under the supervision of Dr. Rashima Mahajan & co-supervision of Dr.Sherin Zafar and has not been submitted in full or part to any other university or institute for degree or diploma. Further, it is certified that short synopsis is plagiarism free and the proof has been submitted.

(Ashu)
17/PhD/038

Signature of the Supervisor
Dr.Rashima Mahajan,
Associate Professor, Department of CSE,
FET, MRIIS (Faridabad)

Signature of the Joint Supervisor
Dr.Sherin Zafar,
Assistant Professor, Department of CSE,
SEST, Jamia Hamdard (New Delhi)

**(Chairman, DRC)**

**Chairperson, CDP**

## ABSTRACT

Ad-hoc networks are the contributors of the wireless technology that have opened new dimensions in the area of research and technology. Such networks do not rely on preexisted infrastructure for linking files between devices through the internet. The necessary procedures in ad-hoc networks are carried out through the help of all existing available nodes. Owing to this integral shortage of setup, the nodes of ad-hoc networks cannot be deliberated as trustworthy in comparison to devoted infrastructure setup. Therefore, there is a need to secure the structure of ad-hoc networks so that basic operations of systems including routing could be performed efficiently. However, these networks are sensitive to various kinds of assaults. Distributed Denial of Service attack (DDoS) is one of the various teething issues which highly overload the resources. The repercussion of such attack will be further effecting routing, Quality of Service (QoS) and security that will further require optimization. In order to optimize security, network must ensure data confidentiality, data integrity, and availability of services. This research synopsis provides a comprehensive outline for selecting secured hybrid routing protocol among the existing protocols based on their comparison analysis under DDoS attack. Research work will primarily focus on developing more efficient hybrid and multipath secured routing protocol for ad-hoc networks. Progressive computational intelligence methodology will be used to enable an analysis of complex security issues for the proposed protocol. Network Simulator (NS) and MATLAB simulation will be utilized for the validation of the proposed approach. This research work aims to optimize different routing, QoS and security issues for performance enhancement of Mobile Ad-hoc Networks (MANET) through hybrid approach. The research proposal would validate the optimization of MANET by overcoming its security issues by applying computational algorithms and comparing the traditional approach with the proposed algorithmic analysis. Proposed work aims to provide effective hybrid and secured protocol to achieve detection and prevention of such attacks. With the advancements in technology brought by Internet of Things (IoT), offering a wide variety of smart devices, security becomes a focal point since devices are heterogeneous in nature. The proposed hybrid protocol will find its application in the IoT based real time applications that are highly prone to DDoS attacks.


**Keywords**: WMN, DDoS attacks, HWMP, AODV, SAODV, Blockchain, and Machine Learning.

**CONTENTS**


| S. No. | Description | Page No. |
|---|---|---|
| 1 | Introduction | 1 |
| 1.1 | DDOS attacks in WMN | 3 |
| 1.2 | Security challenges in networks | 4 |
| 1.3 | Vulnerabilities in complex networks | 5 |
| 2 | Literature Review | 8 |
| 2.1 | Gaps in literature | 12 |
| 3 | Description of Broad Area | 13 |
| 3.1 | Routing protocols for WMN | 14 |
| 4 | Objectives of Research | 18 |
| 4.1 | Problem identification | 18 |
| 4.2 | Objectives of the study | 18 |
| 5 | Methodology | 19 |
| 6 | Expected Outcome of Research | 21 |
| 7 | Proposed Time Frame(Gantt Chart) | 22 |
| 8 | References | 23-27 |

## 1. Introduction

Over the last two decades, wireless networks and mobile computing fields are undergoing dynamic developments. This is credited to the associated advantages of wireless networks in comparison to wired, majorly because of easy scaling; rapid deploy ability and the most significant cost-effective intelligent devices for a better smart world. Many different disjoint research networks have tried to explore different communication technologies for attaining these objectives. A communication between a set of at least two or more devices forms a network in computing. In practice generally, a network comprises of different number of computer arrangements related through physical and wireless links. The services offered by networks vary from a simple task of sharing with basic peripheral devices to enormous data centers situated all over the world. Irrespective of range, all types of networks allow computers along with entities to share data and assets among each other (Mashal et al., 2015).

MANET is a kind of wireless network that does not depend on centralized infrastructure thus, also known as a decentralized form of a wireless network. Ad-hoc networks do not build upon on pre-existing infra like wired network routers or wireless network access points. Each node in ad-hoc networks contributes to routing via transmitting information to several other nodes. Data transmitted by the nodes is determined dynamically depended on network connectivity and routing algorithm being utilized. As ad-hoc network is a decentralized kind of network deployed in a hostile environment, it is inclined to different types of assaults. Therefore, security is an important issue to be handled by networks. Ad-hoc networks include thousands of nodes that are self-organizing in nature, consume low-power and are pocket-friendly because of their low-cost. Such networks are utilized in an assortment of usages including military-related detecting activities along with, monitoring of environmental changes and have wide application in disaster management too (Kaur and Singh, 2017).

Wireless Mesh Network (WMN) is considered not only as self-organized but also as a self-configured network similar to ad-hoc networks. Various devices (laptop, mobile and desktop) often called nodes; communicate information among each other via established mesh topology, to be responsible for connectivity. These mesh nodes includes laptops, mobile phones along with routers, containing Wi-Fi admittance sockets, also known as clients. WMN possesses distributed architecture as shown in figure.1 where different clients in addition to routers connect to distribute the association (Prabha et al., 2015). The significant features and the

benefits of WMNs in delivering network facilities for instance internet access, transferring information through video and voice and transmitting data among networks are coverage, compatibility, mobility, heterogeneity, and scalability (Wu et al., 2017).

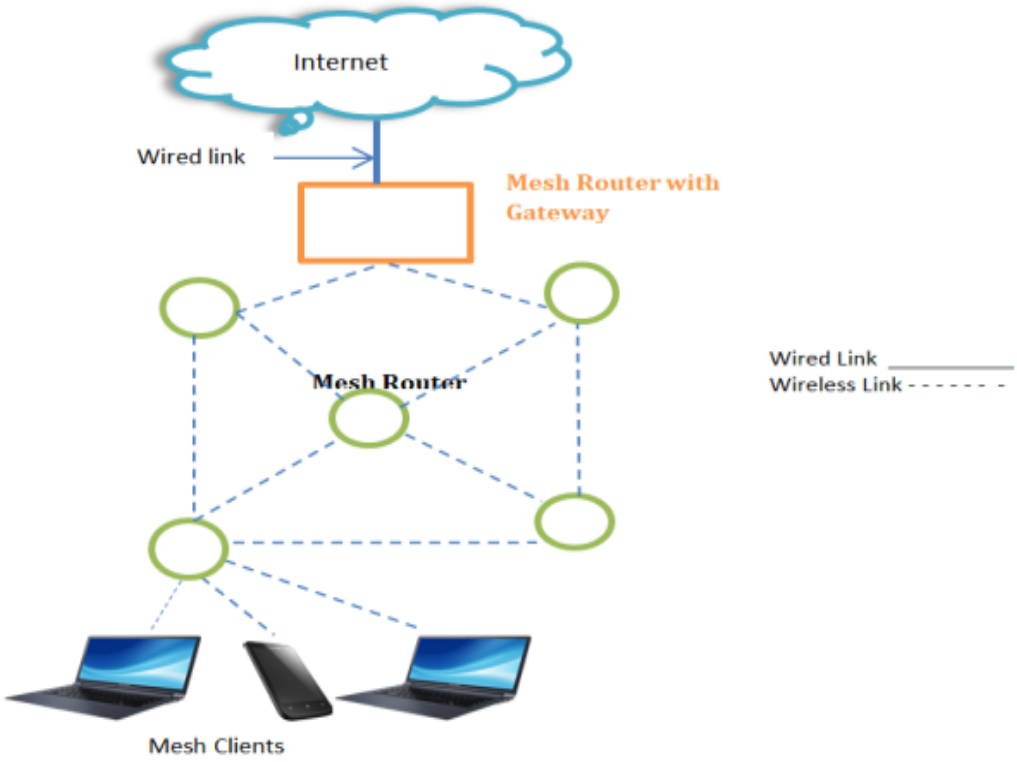



Figure 1: Wireless Mesh Network

Therefore, WMN turns to be a prominent communication innovation in modern time, which embraces multi-hop progressing procedures for speedy information correspondence with the least loss of data. It's rising as an extremely developed communication technology appropriately designed for numerous cyber-physical alliance applications like: smart grids, claims related to defence and for a system based on internet of things (Alippi et al., 2017).WMN is susceptible to several attacks categorized as DDOS, flooding, black-hole and grey-hole because of its multi-hop nature. The repeated broadcast of large quantities of HELLO packets, through the mischievous node is known as flooding attack leading to a denial of service. Jamming is caused at the receiver and further at communication stations of the network, leading to an upsurge of packet dropping ratio, ultimately blocking the

communication. WMN's are apposite for numerous applications in military as well as in civilian fields. Mesh networks gives the best possible solution in various domains where wired communication cannot be done or is dangerous, such as in public safety and wireless system intended for disaster recovery. It deals with easy and quick connectivity over a wireless technology acting as an intermediate. Next subsection focuses upon DDOS attacks occurring in wireless mesh networks.

### 1.1 DDOS attacks in WMN

WMNs are incredibly susceptible to numerous categories of existing attacks because of their intermediate medium, which is universal wireless access and constrained assets. The intended users will be unable to make use of network resources or infrastructure in the presence of such attacks. As the WMN runs on unlicensed 2.4GHz band, the attacker aims to prevent the service from working efficiently either temporally or indefinitely. To reduce network resources through directing a rush of packets from a malicious node (clients and routers) whose number could be one or more, is the focal target of DDOS attack (Vazhayil, Vinayakumar and Soman, 2018). Ultimately this attack causes congestion in the network by injecting a considerable amount of traffic into the system. All the layers (physical layer, link layer, network layer, transportation layer) of WMN are susceptible to these types of attacks. Disseminated refusal of administration could be one of the consequences, i.e., DDOS assaults can cut down your site and abandon you from reaching to the remainder of the web for a considerable length of time or days on end.

Getting the pieces after a DDOS assault is a lengthy and exorbitant procedure. The average money related expense of a DDOS attack for a small or moderate size business is about $123,000, and that number is on the ascent. DDOS assaults have become enormous and progressively complex throughout the years, and they save no site or system. Thirty-three percent of organizations were hit by DDOS assaults in 2017, about twofold the number of assaults in 2016. Eighty-two percent of associations have confronted various DDOS assaults (Dan, 2018).

Routing disruption, along with resource depletion, are the two attacks that could be present in various protocols and are a grave concern in a mesh-based network. Such severe attacks can confess not only the reliability of the paths but also the accessibility of the whole system.

Mischievous nodes possibly can create bad traffic, interrupt as well as alter packets, or refuse to forward packets by merely dropping them. In the presence of protection like end-to-end cryptographic mechanism, a nasty node can descent packets going through it, or influence the network paths by issuing false routing information (Pratomo, Burnap and Theodorakopoulos, 2018). Many researchers have proposed numerous routing protocols to optimize performance of wireless mesh networks. However, there is a severe demand to study the performance features of the routing protocol in WMN's. This research study will provide a comparison analysis based on various performance metrics of reactive protocols; i.e., Ad-hoc on-Demand Vector (AODV) and hybrid protocol; Hybrid Wireless Mesh Networks (HWMP) and will further utilize their performance specific results for optimization in real life scenarios.

### 1.2 Security challenges in networks

With the gradual merging of the Internet with social life, individuals are not only affected by studying and working capacity but are also exposed to gradually severe safety threats. Documenting multiple network attacks, particularly outstanding attacks, is a significant problem that needs to be immediately addressed. Cybersecurity seems to be responsible for technology and is intended to protect personal computers, networks, programs and data from assaults and unauthorized admission, alteration, or harm (Wu, 2017). A structure of network security comprises of a system of personal computer security. Firewalls, antivirus code as well as Intrusion Detection Systems (IDS) are comprised in each system. When developing a safe network, the subsequent considerations must be taken into account:-

- Accessibility: Authorized users have access to and from a specific network.
- Privacy: Network information remains private; the disclosure should not be easily available.
- Authentication: It makes sure that the users of the network are the person they claim to be.
- Integrity: It ensures that the message in transit has not been changed; thus the information is the same as it is sent.
- Non-repudiation: It makes sure that the user does not reject the use of the network.

Safety needs to be incorporated to plan safe networks based on wireless sensors, into each node, which is part of the whole arrangement. That is owing to the probability that the applied component can quickly become attack point in the absence of security. Thus, it means that safety must cover all strategical features of wireless sensor-based network application, which requires high-end security (Azzawi, Hassan and Bakar, 2016). In recent years, wireless sensor systems have received much consideration. The severe energy limitations and the challenging deployment of wireless sensor networks are leading to various security issues in conventional networks. Components of the network system can become an attack point. It is therefore vital to enhance security of each module to encompass security and privacy into all characteristics of the proposal to prevent breaches across various protocols (Mahdavinejad et al., 2018).Real-time based system speculation is one of the global research challenges that depends on actuators and transducers along with the computer based info interchange. For such systems it is necessary to develop a new framework that allows the speculation of salient system options in real-time (Wang, Vetter and Wu, 1997). Along with security, robustness, and safety are the other challenges by which networks are affected. Communication with physical world exhibits uncertainty levels due to the logical calculations happening in cyber systems (Xiao, 2018). The main issues hampering the interactions with physical world are environmental uncertainty, errors in devices, and likelihood of security extortions. Further section 1.3 presents various vulnerabilities occurring in complex networks that becomes the basic goals behind the literature review of section 2.

### 1.3. Vulnerabilities in Complex Networks

Security in networks is continuously developing, owing to traffic growth, usage trends and the ever-varying threat landscape (Zhao et al., 2015).The extensive endorsement of cloud computing, social networking and Bring-Your-Own-Device (BYOD) platforms are bringing up new problems and risks to an already complex network. MANET are susceptible to various network layer assaults due to the remoteness of centralized structure. MANET comprehends several imperfections that make its network prone to multiple attacks and thus, becomes an easy target for attackers. Absence of centralized monitoring of the system posses difficulty to ensure the desired behavior of all the participating nodes. The arbitral movement of the nodes in MANET makes changes unpredictable in the topology. All the participating nodes need the

energy to converse among them. Thus, other primary concern is regarding significant power requirements of the participants. Scalability is one more apprehension in MANET because of movements in nodes which could access network as well as leave independently.

Worm hole, black hole, gray hole, byzantine and sybil attacks are few examples of network layer attacks that devour their configuration, causing loss of information and network deprivation. A node declares itself to have the nearest routes to all destinations in case of black hole attack. Network performance gets degraded as this node grips entire data packets in the routing protocol (Li, Yan and Fu, 2018).

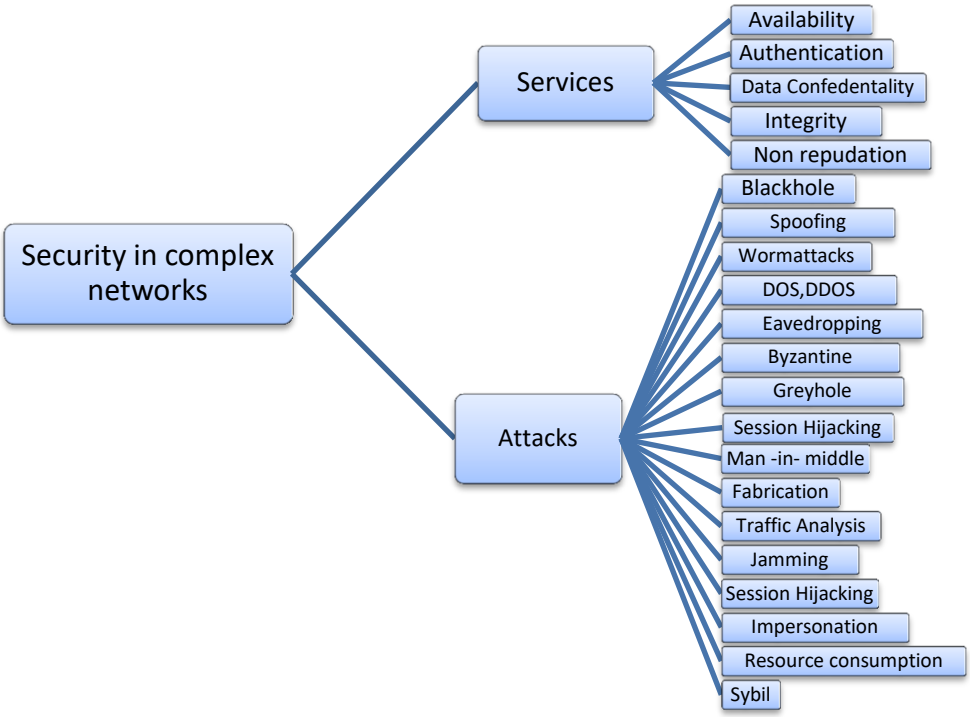



Figure 2: Security Aspects in Complex Networks

Eavesdropping states to attack when an opponent can capture any evidence transferred by the arrangement. The attacker in this attack never interferes with the functioning of the system and only notices its process, thus it is the so-called passive attack. Complex systems like Cyber Physical System (CPS) are mainly vulnerable to eavesdropping via traffic examination, for instance, intercepting the monitoring of records transmitted in networks of sensors collected through tracking. It also affects users privacy, such as information on the health status

transferred in the scheme. Figure.2 represents various categories of attacks; eavesdropping attacks are the most likely occurring on data aggregation procedures.

In compromised-key attack a key as a unique code is essential for acknowledging safe data. Once the attacker finds a key, a compromised key is deliberated (Alvarez, Maag and Zaidi, 2017). Through the negotiated key, an intruder can access a protected communication deprived of the sender or receiver consciousness. The attacker can alter data by the conceding key, and attempt to use the compromised one to calculate furthermore keys, which possibly could permit the attacker admittance to new secured infrastructures or resources. In man-in-the-middle attack, factually incorrect messages are addressed to the recipient. In this sort of assault messages may take either category of a false negative or a false positive. This may lead the operator to initiate unnecessary activities, such as breaker flipping, when it is not essential, or may also lead the operator to consider everything to be okay and therefore not to captivate an action when action is needed.

Denial-of-service attack eludes the arrangement from handling real traffics or requests for network assets. It classically transmits an enormous quantity of information to the network to mark the hectic management of data so that normal facilities cannot be delivered. The attacker can always do any of the following steps after entering the network: firstly it floods the entire sensor network with traffic until a shutdown occurs due to the overload. Secondly, it will direct invalid information to the controller or system as a result of which facilities/services are unusually revoked or treated.

Introduction section of the synopsis has focussed on concepts of networks and attacks, further in section 2 relevant analysis has been done on the various researches carried over for tackling security in WMN and MANET. Section 3 depicts broad area that focuses on various protocols of MANET and WMN, their benefits and demerits have also been discussed and hybrid protocols are compared. Section 4 includes objectives of proposed research followed by methodology in section 5.The expected outcomes of research are listed in section 6, followed by gantt chart depicting the time frame for completing the research work in section 7 and references are listed in the end as section 8.

## 2. Literature Review

Relevant analysis attends to the various investigations carried out in the security field for numerous categories of attacks in different types of complex networks. Studies carried on complex networks for a finding of attacks could be classified as for improving the routing protocol. Thus, the comparison of reactive and hybrid routing protocol becomes the foundation of the planned research work. Several latest papers are analysed by exploring computational intelligence principles for providing security and trustworthiness in various fields of routing protocols. Various related work of different authors is analyzed for finding gaps of study.

Various researchers have analyzed network performance under black hole attack through NS by taking into considering most popular AODV protocol. Network conditions were simulated with dissimilar affecting speeds, different quantities of communication and malicious nodes. For improved simulation of real time networks, random features are analysed to attain the arbitrariness of communication entities. The investigational results display several influences of blackhole attacks on QoS factors such as packet loss rate, average throughput and average end-to-end delay, which endorse the investigation of MANET security measures (Li, Yan and Fu, 2018).

Researchers through attack model aimed at IoT structures, reviewed the IoT security answers grounded in the approach of machine learning comprising supervised, unsupervised plus reinforcement learning (Whitmore, 2015).

Machine learning-centered IoT authentication, admittance control, secure offloading as well as malware detection arrangements were focussed in this research study. It was highlighted that standby security mechanisms have to be provided to guard IoT systems from the investigation stage in the learning development (Arel, 2010).

Authors have discussed the framework inclined to the chief features of security in wireless sensor networks focussing on attacks and its categorization mechanisms. Due to inimical characteristic of WSN environments, presence of wireless medium along with the inhibited characteristics of resources of tiny sensor devices incorporated in such networks, security poses additional severe challenges in comparison to traditional networks. Attacks in some part of the hardware or software might offer vital compensations in those networks. Certainly, the growth

of operative and effective protection mechanisms to attacks need to be addressed at each phase of the structured plan (Chelli, 2015).

Authors analysed machine learning-centred plan to identify attacks specifically spoofing in WSN, creating wide-ranging methodical models. The suggested algorithm conglomerates double classifiers to route as well as to examine the immediate samples of customary signal strong point to spot attacks. The proposed algorithm is improved for scenarios where the honest node and the attacking node are at the equal distance or at a close distance from each other concerning the landmark, which is the nastiest case situation. The outcomes specify that the proposed approach mends the routine of the attack detection to about 10% when compared to an alike method in literature (Mohammadi et al., 2018).

This research study specifies the current difficulties of security in IoT networks and indicates the requirements of intrusion detection (Zhou et al., 2018).Numerous types of Intrusion Detection System (IDS) tools were deliberated, and its solicitation on IoT architecture was investigated. The applications of diverse intrusion detection technologies were inspected in this research. A specific class characteristic or a detection model poses difficulties to analyze detection rate of network IDS. The performance of the projected model is confirmed via public databases. Emphasis was given on the machine learning-based approach along with the exhausting data mining for studying the network intrusion technology, which has great potential in the future(Zeng, Guo and Cheng, 2011).

Learning the consequence of amount heterogeneity on fundamental susceptibility of co-dependent networks, when they agonize beset attacks was emphasized in this research work. The hypothesis specifies an interdependent arrangement model composed of dual network components. The degree of heterogeneity of each network can be controlled by controlling its QoS parameters (Wang, Vetter and Wu, 1997).

An Insight of IoT procedure in smart health care and the contributions of IT in managing the enormous volume of high-security patient's medical information is detailed in this research work. The depth of interconnection is an addition in healthcare, as factors influencing health, both external & internal to the human body may perhaps be analysed established on the model (Yeh, 2016).

This research work focusses on an advanced design of a network that is based on software-defined set-up offering a network controller via software-based reasoning. To modify the

network according to the user needs it decouples both the control and data plane. A uniform network protocol called open flow becomes an interface amongst different controllers and switches. The software-based supervisors are extremely susceptible to distributed denial of service attacks. The stochastic Restricted Boltzmann Machine (RBM) algorithm unsupervised in nature was used for finding system to self-learn all the trustworthy network metrics. This set of rules distinguishes and categorizes types of DDoS attacks in a vibrant network surrounding a new framework. The outcomes confirm that RBM based DDoS exposure system attains higher accuracy in comparison to the prevailing approaches (Mohana Priya et al., 2017).

Authors(Wang, 2005) have carried a research study network layer is trusted as the most significant part of comprehending IoT environment and indorsed as a well-designed network for supervision, connection administration, grouping and confidentiality. The most stated machine learning algorithms includes: support vector machine, artificial neural network, naive bayes, decision tree, knn, k-mean, random forest and deep learning (Meng et al., 2017). For handling security in IoT networks it has been proved that Support Vector Machine (SVM) is the most widely used machine learning technique and is also used in important studies both for intrusion detection as well as for authentication. It is one of the supervised learning technique that produces (either of classification or regression function) mapped input-output functions from characterized training data set.

To bridge the gap between analytics and learning in the field of IoT, Deep Learning (DL) algorithm is utilized in this research study. The prospective research study utilizes DL techniques for IoT information analytics and its potentials and dares are presented (Sokolov, Pyatnitsky and Alabugin, 2018).

A novel structure called pigeon principle and hybrid encryption headed for sensing and overcoming the flaw named watchdog discussed in this study encounters various problems in MANET like: partial dropping, complexity and ambiguous impacts, which have not been taken care by other existing research schemes. Planning of hybrid encryption structure, as well as pigeon principal, disables all the weakness of watchdog. Receiver collision have also been identified and sensed by Enhanced Adaptive Acknowledgement (EAACK) thus giving a good outcome. However, there is a need to improve the rate of data transmission that needs to be considered along with complete energy harvesting (Sridevi and Nagarajan, 2017).

The networks based on IEEE 801.15.4 standard were taken into care for evaluating the performance of three routing protocols namely AODV, second Optimized Link State Routing (OLSR) and Zone Routing Protocol (ZRP) for the occurrence of attacks categorized as wormhole. The parameters accustomed to understand the performance of different reactive (AODV), proactive (OLSR) and hybrid (ZRP) routing protocols in networks are average end-to-end delay, Packet Delivery Ratio (PDR) and energy consumption in sensor networks. In this research work qualnet simulator 5.0 was used for simulation. Throughput was highest in ZRP while OLSR had lowest average end-to-end delay. AODV improved total throughput and end-to-end delay when compared to ZRP and OLSR (Kaur and Singh, 2017).

Researchers emphasized on necessity of secured protocol for routing and energy-efficient IDS to avoid dangers in wireless networks (Brill and Nash, 2017).

A theoretical block chain -centered conceded firmware recognition and self-healing tactic were discussed in this research paper, which has set up in IoT environs. Authors have mentioned four different directions in which block chain could be used, one of which is to explore the usage of block chain as a collaborative security foundation to secure other networks of IoT, or other networks or systems, for example, cyber-physical system. Further, it has been emphasized and concluded that there is a strong need to explore the optimization of block chain and also about the different platforms available for block chain implementation (Banerjee, Lee and Raymond Choo, 2018).

After performing an intense literature review, it has been observed that there are various advantages and disadvantages of gradual inclusion of internet and social life. The online world not only changes the way individuals learn and operate, but it also exposes them to severe protection threats. The motivation to carry the proposed research is to overcome various existing problems in the traditional protocols and algorithms which have been identified in the literature survey. A need is there to propose and implement more efficient security protocols taking into consideration various optimization and machine learning platforms.

## 2.1 Gaps in literature

An extensive literature analysis in the previous section has led to the identification of the gaps that needs to be addressed. Research analysis below presents various gaps in study that will lead to problem formulation which will be discussed later in this synopsis:

1. Research studies highlight that DDOS type attacks cause serious damage to the performance of any network and should be strictly prevented. So revealing of a nasty node in the MANET based network is the prime-most concern of the proposed study.
2. Unavailability of efficient existing algorithms to identify the destructive nodes along the network.
3. Network effected with attacks facade drawbacks; less throughput, low packet delivery ratio, high network routing overhead etc. Network small in structure are more susceptible to various types of attacks and consequently leads to various security breaches.
4. The criteria for the effectiveness of the intrusion detection system can be achieved by the different computational intelligence characteristics, typically adaptation, fault tolerance, fast computational rate plus error resilience in the noisy data aspect. However the best possible solutions have not been discussed yet. Thus, there is a need to provide an optimal solution by applying computational methods to tackle security-related issues by evidently describing present research.

Problem formulation will specify various consequences of analysis that will deliver valuable visions into existing security work thus, becoming the foundation for applying computational approaches in hybrid routing protocol of MANET on favorable new instructions for research.

## 3. Description of Broad Area

This section briefly describes the broad area of research analysis. The enormous growth of the internet has led to greater awareness and attention in network security and routing. Three-level internet security needs have been recognized: Quality of Service (QoS), secure network structure and security of the end system (Chelli, 2015). End system security is classically achieved by setting up a post security barrier and new firewall technology is utilized to expand "defense perimeter" by protecting internet and intranet for various organizations with a trivial amount of firewall systems. End-to-end security is well suitable to offer confidentiality, authentication and integrity. Protected QoS presents a numeral of novel security challenges: authentication and authorization of operators who require affluent network assets, mutually to prevent resource holdup and to avoid denial of service due to unapproved traffic, etc. Network action determined by management and control conventions establishes and operates network infrastructure, routers, DNS servers, etc.

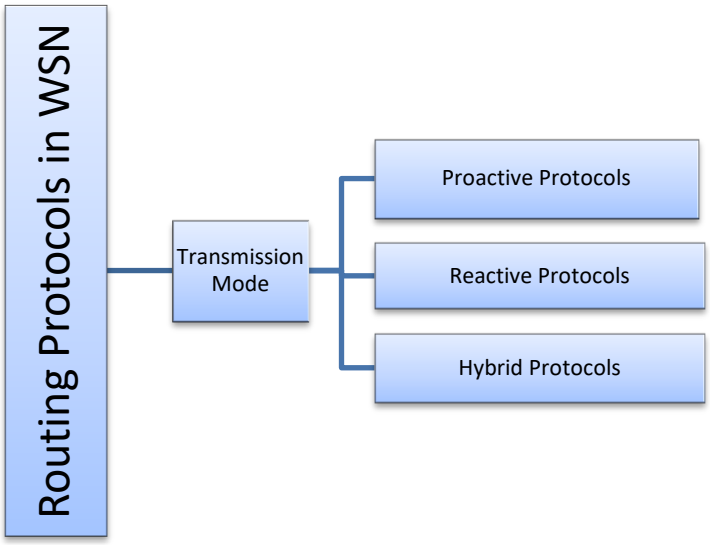



Figure 3: Categorization of Routing Protocols in Sensor Networks

An influence on system arrangement can cause denial of service from the user's viewpoint, however for network engineer; the invader is taking benefit of the absence of authenticity, integrity and perhaps privacy (Spaulding and Mohaisen, 2018). Figure.3 shows the categorization of routing protocols in WSN. These protocols are intended to meet modest network letdowns (for example, links up-down, echoing and restarting nodes, etc.) thus, can

have numerous susceptibilities when facing purposely positioned assailant (Govindasamy and Punniakody, 2017). In the upcoming subsection routing protocols for WMN are analyzed.

### 3.1. Routing protocols for WMN

Routing protocols are categorized as proactive, reactive and hybrid based on their respective features.

a) Proactive or Table-Driven Protocols

In these protocols, paths are well-defined in table. With each change in network configuration the routes are updated (Kaur and Singh, 2017). Routes are restored by sending a broadcast message to complete network. In proactive routing, overhead is more because of upholding of updated route, however the delay is less due to already defined routes in the table. Since they preserve routing information even before it required they are termed proactive. Such protocols are not appropriate for big networks as they preserve node entry individually for every node in the routing table. DSDV, OLSR and Wireless Routing Protocol (WRP) are some examples of such routing protocols (Sanzgiri et al., 2002). OLSR is improved for MANET systems, which possesses similar characteristics like that used for WSN (Yeh et al., 2016). It enables efficient flooding of control communication across the network through chosen nodes known as Multipoint Relays (MRPs).The issues of flooding the network is overcome by MRP nodes through control memorandums. MRPs are nominated by each node as well as are used to forward control memos ensuing in dispersed process of the rules. Along with this, a node endlessly upholds paths to all endpoints of network, thus creating the rules suited for traffic design that is arbitrary and irregular. Also, proactive feature make OLSR appropriate for networks that modify interactive sets over time. This protocol is an optimization of traditional MRP routing algorithm. The mentioned protocol is also capable of movement sorts operating with another huge sub-set of substations in a massive sub-set of nodes, and wherever the origin and destination strands change over time. For huge and dense networks, it is predominantly well matched (Deng et al., 2017).

b) Reactive or On-Demand Routing Protocols

Reactive protocols explore routes on demand. Such protocols have fewer overheads and delays. The route is revealed through flooding the Route Request (RREQ) packets over the complete network (Brill and Nash, 2017).AODV usages an on-demand method to catch routes, i.e. a route is only set when a source node is obligatory to transmit information packets. AODV has two tranquil processes for discovering and preserving path. Route Request (RREQ), Route Reply (RREP) and Route Error (RERR) communications are used by AODV to detect and keep routes. It communicates an RREQ packet to the network after a source node demands way to the endpoint node for which it does not have a path. An RREQ packet comprises of the IP source, IP address, source sequence number, destination sequence number, request ID and hops count. If a node accepts a route demand with the identical source address and requests ID fields as in former route demand packets, the packet will be rejected. Else, it will inspect whether there is an access for the endpoint address in its routing table. If an address is available, the endpoint protocol number in the table is connected with an endpoint in its routing table and if it is unable to extend the endpoint through that path, it raises the endpoint sequence number and sends a request for a path. Therefore, the endpoint sequence number indicates route's freshness. In path preservation, when link is damaged in an active route, the node informs this link breaking by directing a RERR communication to the source node. It will reinitiate its path detection procedure for sending the information.

c) Hybrid Routing Protocol

Hybrid protocols conglomerates features of proactive and reactive protocols for achieving enhanced results. Such routing protocols fix the overhead routing of proactive processes and postpone reactive processes. In this, networks are separated into zones and appropriate for large networks. Hybrid protocols practice reactive routing, for route discovery scenario. However, for table maintenance process the proactive protocols are widely utilized by hybrid routing protocols. The kind of hybrid routing protocols that are most widely used for discovering routes are: ZRP, Hybrid Clustering Routing (HCR) and Ant based Hybrid routing algorithm for mobile and adhoc networks (ANTHOCNET). Hybrid protocols are an innovative group of procedures, an amalgamation of both proactive and reactive protocols. They have the prospective to deliver higher scalability in comparison to pure reactive or proactive protocols. Additional originality of hybrid routing procedures is that to establish the network in accord

with network parameters (Sengupta, Sengupta and Das, 2017).Hybrid procedures can deal with greater scalability in comparison to the traditional two classes.

**Table 1: Hybrid Secured Routing Protocols**

| Protocols | Parameters | | | | |
|---|---|---|---|---|---|
| | Multiple Routes | Routes Information Stored in | Route metric | Advantages | Disadvantages |
| ZRP (Sharma, and Trivedi, 2016) | No | Tables for Intra zone region & Inter zone region | Smallest route | Reduced transmissions | Overlapping zones |
| ZHLS (Alvarez, Maag, and Zaidi, 2017) | Yes | Intra zone & Inter-zone tables | Smallest route | Low control overhead | Static zone map required |
| DST (Sharma, Sharma and Kalia, 2016) | Yes | Route tables | Progressing using tree table | Reduced transmission | Root node dependency |
| DDR (Walikar and Biradar, 2017) | Yes | Intra zone & Inter-zone tables | Stable routing | No zone controller | Neighbors may become a bottleneck |
| Anthocnet (Walikar and Biradar, 2017) | Yes | Pheromone & neighbour table | Using pheromone | High delivery ratio, robustness, adaptable, scalable | No centralized processor to guide the system towards a good solution |
| HCR (Walikar and Biradar, 2017) | Yes | Host clustered list, Member node list, Neighbour cluster list, global cluster table | ELECT_CH(cluster head),INTRA_CB,INTER_CB(for global cluster table GCT) | Headset approach, less overhead delay | Cluster head changes are expensive, cluster head CH selection, Imbalance of energy consumption |
| HWMP (Walikar and Biradar, 2017) | Yes | Tree-based routing maintains the topology | Airtime, packet delivery fraction and delay | It allows nodes to quickly obtain routes for new destination, nodes decide/select own back-up paths | Resource and power wastage problem because of root constraint and tree-based communication |

To decrease the numbers of re-broadcast nodes, hybrid protocols utilize the description of an area, which helps nodes to function together. The most suitable nodes can then be used to determine the route. Thus hybrid protocols attempts to eliminate single point of failures.

## 4. Objectives of the Research

After performing an intense literature review and discussing broad area of research objectives of current study are highlighted in this section.

### 4.1 Problem identification

Literature review reveals that efficient implementations of hybrid protocols need to address DDOS attacks in WMN with higher accuracy, reduced complexity and packet delay should be taken into consideration. The problem of the proposed research is to implement a hybrid multipath routing protocol in WMN and to optimize their security performance by identifying attacker nodes and eliminating average packet delay, by further optimizing their QoS parameters.

### 4.2 Objectives of the study

The prime objective of the research work is to carry out the optimization of security in hybrid networks using computational intelligence. The goal is achieved by breaking the work into the following objectives:

- **(i)** To focus on DDoS attack and its security vulnerabilities in ad-hoc networks and also to study limitations of various traditional security approaches in networks.
- **(ii)** To implement HWMP (Hybrid Wireless Mesh Protocol) and compare its performance with SAODV under DDoS attack.
- **(iii)** To evaluate the performance of multi path HWMP protocol using computational intelligence with respect to SAODV.
- **(iv)** To propose a secured multipath HWMP approach using block chain algorithm and evaluate its performance against DDOS attack.
- **(v)** To detect and classify the attacker nodes of the network with help of computational techniques.

## 5. Methodology

Previous sections elaborated broad of area of research and objectives of study are focus upon WSN of MANET, their securities vulnerabilities, attacks and computational approaches that are implied on these network. With a rising interest in security owing to the increase in internet usage in a smart world, there arises a need for efficient and secure optimization of security in hybrid networks. The proposed algorithm in this synopsis will focus on the application of computational intelligence algorithm to optimize network performance. The proposed algorithm aims to identify the destructive node according to the behavior of nodes present in the system by adopting a secured mechanism based on the block chain concept.

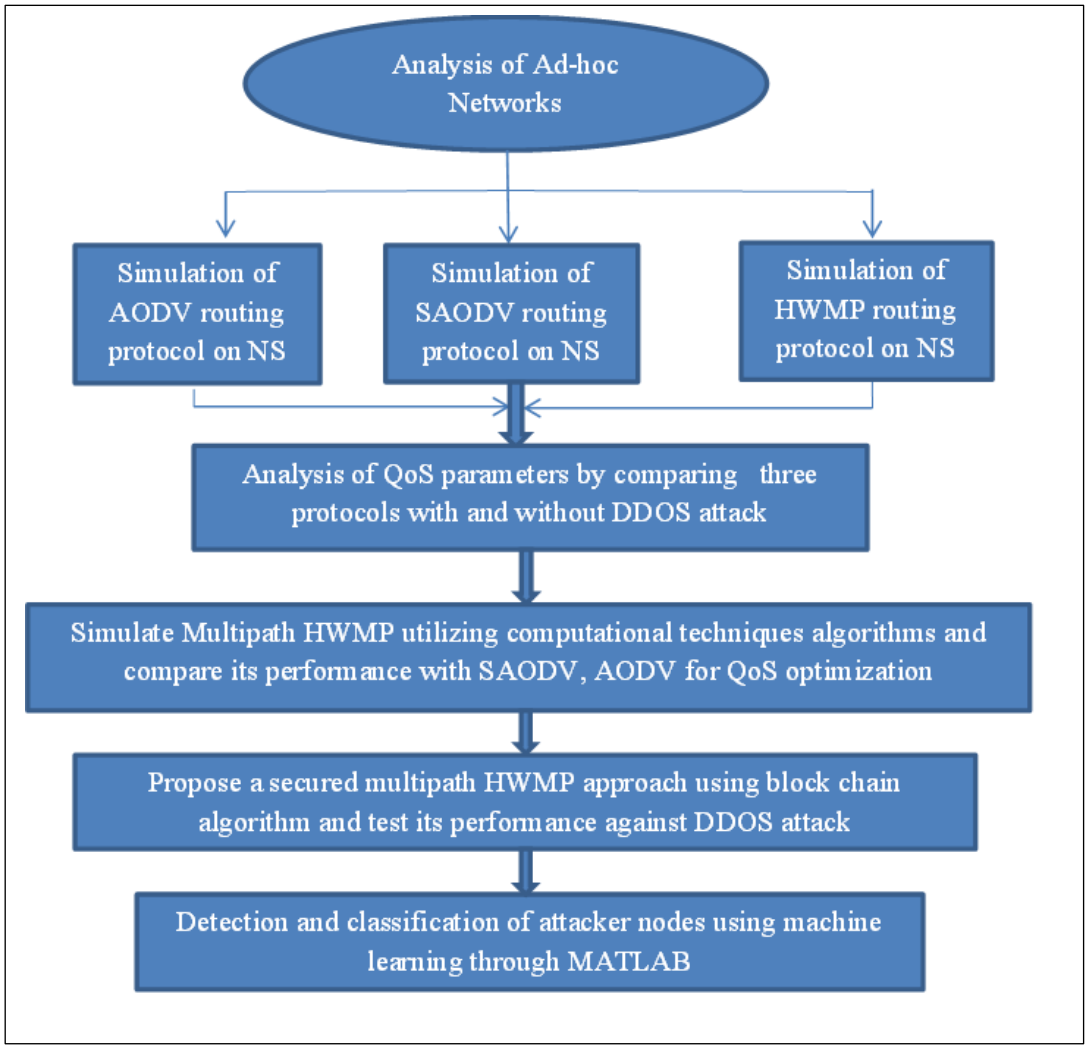

Analysis of Ad-hoc Networks
Simulation of AODV routing protocol on NS
Simulation of SAODV routing protocol on NS
Simulation of HWMP routing protocol on NS
Analysis of QoS parameters by comparing three protocols with and without DDOS attack
Simulate Multipath HWMP utilizing computational techniques algorithms and compare its performance with SAODV, AODV for QoS optimization
Propose a secured multipath HWMP approach using block chain algorithm and test its performance against DDOS attack
Detection and classification of attacker nodes using machine learning through MATLAB

Figure 4: Proposed Methodology Flowchart

The proposed research works as shown in figure. 4, will perform an intense analysis of AODV, SAODV and HWMP routing protocols to compare the reactive and hybrid routing strategy under the condition of DDoS attacks and without DDoS attacks. The next work of the proposed analysis will simulate multipath, HWMP for QoS optimization using deep learning and machine learning-based algorithm and comparing its performance with SAODV and AODV. The third step proposes a secure mechanism using block chain methodology and also tests its performance with DDoS attacks. Final step will detect and classify attacker nodes using machine learning algorithm through MATLAB simulator

Various phases of research modules will be implemented for fulfillments of all the objectives to optimize security through NS are described below:-

Phase1: Proposed analysis based on DDoS mitigation will be implemented and evaluated for its efficiency using NS.

Phase 2: By using the network trace, the performance of the method for DDoS mitigation will be measured. The performance of proposed model will be evaluated through various QoS parameters. The comparison will be made between HWMP and SAODV routing protocol based on their result analysis.

Phase3: Block chain algorithm will be proposed for identifying the attacker nodes with the help of NS. In several applications, the data attained from the sensing nodes could be false, or in other words that node could be malicious node as it could seize private information or could send false messages to other nodes in the network itself. A secured multipath HWMP approach using block chain algorithm will be evaluated against DDOS attack. The focused area of the proposed routing protocol will increase the network security of the adhoc networks. Simulation through NS will validate the developed algorithms taking into consideration various evaluated parameters.

## 6. Expected Outcome of Research

It is being planned to implement in the proposed approach,

- An efficient secure multipath HWMP technique utilizing block chain algorithm for tackling the security of the networks.
- Detection and classification of the attacker nodes present in the network, to solve the problems of intrusion detection in mobile adhoc networks using computational intelligence methods to resolve intrusion detection problems.
- To develop a complete secured, QoS and efficient routing based optimized protocol for MANET by utilizing newest secured approaches mainly block chain and computational algorithms.
- Future development of the algorithm will be depending on the results after simulation and analysis.

## 7 Proposed Time Frame (Gantt chart)

Gantt chart below depicts the time frame for completion of research study.

| **Time Frame** → | **JAN to JUN 2018** | | | **JUL to DEC 2018** | | | **JAN to JUN 2019** | | | **JUL to DEC 2019** | | | **JAN to JUN 2020** | | | **JUL to DEC 2020** | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Months** | 2 | 4 | 6 | 8 | 10 | 12 | 14 | 16 | 18 | 20 | 22 | 24 | 26 | 28 | 30 | 32 | 34 | 36 |
| Course work | | | | | | | | | | | | | | | | | | |
| Extensive literature search | | | | | | | | | | | | | | | | | | |
| Problem statement formulation | | | | | | | | | | | | | | | | | | |
| Publication on literature survey | | | | | | | | | | | | | | | | | | |
| Implement HWMP (Hybrid Wireless Mesh Protocol) and compare its performance with SAODV with DDoS attack | | | | | | | | | | | | | | | | | | |
| Publication on HWMP to eliminate DDoS attack | | | | | | | | | | | | | | | | | | |
| Implement multipath HWMP utilizing machine learning algorithms and compare its performance with SAODV | | | | | | | | | | | | | | | | | | |
| Algorithm development for Secured Multipath HWMP approach using block chain algorithm and test its performance against DDOS attack | | | | | | | | | | | | | | | | | | |
| Publications on DDoS attacks handled by block chain algorithm , report writing and Submission | | | | | | | | | | | | | | | | | | |
| Detection and classification of attacker nodes using machine learning | | | | | | | | | | | | | | | | | | |
| Long synopsis thesis writing and submission | | | | | | | | | | | | | | | | | | |

## 8. References


Alippi, C., D'Alto, V., Falchetto, M., Pau, D. and Roveri, M., 2017, May. Detecting changes at the sensor level in cyber-physical systems: Methodology and technological implementation. In *2017 International Joint Conference on Neural Networks (IJCNN)* (pp. 1780-1786). IEEE.

Alvarez, J., Maag, S. and Zaidi, F., 2017, March. Monitoring dynamic mobile ad-hoc networks: A fully distributed hybrid architecture. In *2017 IEEE 31st International Conference on Advanced Information Networking and Applications (AINA)*(pp. 407-414). IEEE.

Arel, I., Rose, D.C. and Karnowski, T.P., 2010. Deep machine learning-a new frontier in artificial intelligence research. *IEEE computational intelligence magazine*, *5*(4), pp.13-18.

Azzawi, M.A., Hassan, R. and Bakar, K.A.A., 2016. A review on Internet of Things (IoT) in healthcare. *International Journal of Applied Engineering Research*, *11*(20), pp.10216-10221.

Brill, C. and Nash, T., 2017, December. A comparative analysis of MANET routing protocols through simulation. In *2017 12th International Conference for Internet Technology and Secured Transactions (ICITST)* (pp. 244-247). IEEE.

Chelli, K., 2015, July. Security issues in wireless sensor networks: Attacks and countermeasures. In *Proceedings of the World Congress on Engineering* (Vol. 1, No. 20).

Dan, K., 2018.Kaspersky-*B2B"IT Security Risks Survey 2017*". https://www.msspalert.com/cybersecurity-research/kaspersky-lab-study-average-cost-of-enterprise-ddos-attack-totals-2m/

Deng, L., Li, D., Yao, X., Cox, D. and Wang, H., 2018. Mobile network intrusion detection for IoT system based on transfer learning algorithm. *Cluster Computing*, pp.1-16.

Fu, Y. and Ding, Z., 2017, October. Hybrid channel access with CSMA/CA and SOTDMA to improve the performance of MANET. In *2017 IEEE 17th International Conference on Communication Technology (ICCT)* (pp. 793-799). IEEE.

Govindasamy, J. and Punniakody, S., 2017. A comparative study of reactive, proactive and hybrid routing protocol in wireless sensor network under wormhole attack. *Journal of Electrical Systems and Information Technology*.

Kaur, J. and Singh, G., 2017, September. Hybrid AODV algorithm for path establishment in MANET using bio inspired techniques. In *2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI)* (pp. 823-829). IEEE.

Kaur, H. and Singh, J., 2017. COMPARATIVE ANALYSIS OF HYBRID ROUTING PROTOCOLS ZRP, HCR AND ANTHOCNET. *International Journal of Advanced Research in Computer Science*, *8*(7).

Li, G., Yan, Z. and Fu, Y., 2018, May. A Study and Simulation Research of Blackhole Attack on Mobile AdHoc Network. In *2018 IEEE Conference on Communications and Network Security (CNS)* (pp. 1-6). IEEE.

Mahdavinejad, M.S., Rezvan, M., Barekatain, M., Adibi, P., Barnaghi, P. and Sheth,

A.P., 2018. Machine learning for Internet of Things data analysis: A survey. *Digital Communications and Networks*, *4*(3), pp.161-175.

Mashal, I., Alsaryrah, O., Chung, T.Y., Yang, C.Z., Kuo, W.H. and Agrawal, D.P., 2015. Choices for interaction with things on Internet and underlying issues. *Ad Hoc Networks*, *28*, pp.68-90.

Meng, F., Fu, Y., Lou, F. and Chen, Z., 2017, December. An effective network attack detection method based on kernel PCA and LSTM-RNN. In *2017 International Conference on Computer Systems, Electronics and Control (ICCSEC)* (pp. 568-572). IEEE.

Mohammadi, M., Al-Fuqaha, A., Sorour, S. and Guizani, M., 2018. Deep learning for IoT big data and streaming analytics: A survey. *IEEE Communications Surveys & Tutorials*, *20*(4), pp.2923-2960.

Prabha, R., Krishnaveni, M., Manjula, S.H., Venugopal, K.R. and Patnaik, L.M., 2015. QoS Aware Trust Metric based Framework for Wireless Sensor Networks. *Procedia Computer Science*, *48*, pp.373-380.

Pratomo, B.A., Burnap, P. and Theodorakopoulos, G., 2018, June. Unsupervised Approach for Detecting Low Rate Attacks on Network Traffic with Autoencoder. In *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)* (pp. 1-8). IEEE.

Sanzgiri, K., Dahill, B., Levine, B.N., Shields, C. and Belding-Royer, E.M., 2002, November. A secure routing protocol for ad hoc networks. In *10th IEEE International Conference on Network Protocols, 2002. Proceedings.* (pp. 78-87). IEEE.

Sengupta, A., Sengupta, D. and Das, A., 2017, November. Designing an enhanced ZRP algorithm for MANET and simulation using OPNET. In *2017 Third International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN)* (pp. 153-156). IEEE.

Sharma, A.K. and Trivedi, M.C., 2016, February. Performance comparison of AODV, ZRP and AODVDR routing protocols in MANET. In *2016 Second International Conference on Computational Intelligence & Communication Technology (CICT)* (pp. 231-236). IEEE.

Sharma, R., Sharma, T. and Kalia, A., 2016. A comparative review on routing protocols in MANET. *International Journal of Computer Applications*, *133*(1), pp.33-38.

Singh, B. and Singh, T., 2017, March. Modified EGSR for network security. In *2017 51st Annual Conference on Information Sciences and Systems (CISS)* (pp. 1-7). IEEE.

Sridevi, N. and Nagarajan, V., 2017, April. Enhanced secure wireless communication in MANETs. In *2017 International Conference on Communication and Signal Processing (ICCSP)* (pp. 2256-2261). IEEE.

Sokolov, A.N., Pyatnitsky, I.A. and Alabugin, S.K., 2018, November. Research of Classical Machine Learning Methods and Deep Learning Models Effectiveness in Detecting Anomalies of Industrial Control System. In *2018 Global Smart Industry Conference (GloSIC)* (pp. 1-6). IEEE.

Spaulding, J. and Mohaisen, A., 2018, October. Defending Internet of Things Against Malicious Domain Names using D-FENS. In *2018 IEEE/ACM Symposium on Edge Computing (SEC)* (pp. 387-392). IEEE.

Vazhayil, A., Vinayakumar, R. and Soman, K.P., 2018, July. Comparative Study of the

Detection of Malicious URLs Using Shallow and Deep Networks. In *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)* (pp. 1-6). IEEE.

Walikar, G.A. and Biradar, R.C., 2017. A survey on hybrid routing mechanisms in mobile ad hoc networks. *Journal of Network and Computer Applications*, *77*, pp.48-63.

Wang, F., Vetter, B. and Wu, S.F., 1997. *Secure routing protocols: Theory and practice*. Technical report, North Carolina State University.

Whitmore, A., Agarwal, A. and Da Xu, L., 2015. The Internet of Things—A survey of topics and trends. *Information Systems Frontiers*, *17*(2), pp.261-274.

Wu, Y., Sun, S., Wang, L. and Xia, C., 2017. Attack vulnerability of interdependent local-world networks: The effect of degree heterogeneity. In *IECON 2017-43rd Annual Conference of the IEEE Industrial Electronics Society* (pp. 8763-8767).IEEE.

Xiao, L., Wan, X., Lu, X., Zhang, Y. and Wu, D., 2018. IoT security techniques based on machine learning. *arXiv preprint arXiv:1801.06275*.

Zhao, Z., Ding, W., Wang, J. and Han, Y., 2015. A hybrid processing system for large-scale traffic sensor data. *IEEE Access*, *3*, pp.2341-2351.

Zhou, W., Jia, Y., Peng, A., Zhang, Y. and Liu, P., 2018. The effect of iot new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. *IEEE Internet of Things Journal*, *6*(2), pp.1606-1616.

MANAV RACHNA
Vidyaprateekshate

**Dr. O.P. Bhalla Central Library**
**Manav Rachna International Institute of Research and Studies**
*(A deemed to be university under section 3 of UGC Act 1956)*

# SIMILARITY VERIFICATION CERTIFICATE

Title: Optimization of Security in Hybrid Networks using Computational Intelligence

Researcher: Ashu Registration Number: 17/PhD/038

Supervisor: Dr. Rashima Mahajan Department: ECE

This is to certify that the above mentioned Short Synopsis/Thesis was scanned for similarity index through Turnitin Software on 25 Sep. 2019 with submission ID 1179737813 and the similarity index was found to be 7 %. The complete report running into 33 Pages, 7443 Word count with File Size 6665 KB is being forwarded to the Research Supervisor/DRC/DRB for review.

Date: 15.4.2021

The complete report of the above Short Synopsis/Thesis has been reviewed and the similarity index is below the accepted norms as per the University Grants Commission (Promotion of Academic Integrity and Prevention of Plagiarism in Higher Educational Institutions) Regulations 2018. The Short Synopsis/Thesis may be considered for further processing

Research Scholar

Research Supervisor

# SHORT SYNOPSIS

*by* Ashu 1 Abc

**Submission date:** 25-Sep-2019 05:56PM (UTC+0530)
**Submission ID:** 1179737813
**File name:** synopsis_for_Ashu_sep25,2019.docx (223.97K)
**Word count:** 7443
**Character count:** 42775

# Optimization of Security in Hybrid Networks using Computational Intelligence

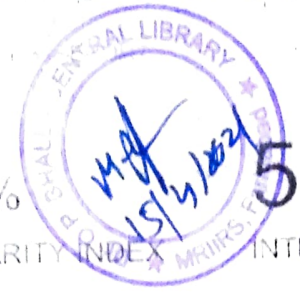
## SHORT SYNOPSIS

Ashu
Registration number: 17/PhD/038

## ABSTRACT

Ad-hoc networks are the participants of the wireless technology that have opened new dimensions in the area of research and technology. Such networks do not rely on preexisted infrastructure for linking files between devices through the internet. The necessary procedures in ad-hoc networks are carried out through the help of all existing available nodes. Owing to this integral shortage of setup, the nodes of ad-hoc networks cannot be deliberated as trustworthy in comparison to devoted infrastructure setup. Therefore, there is a need to secure the structure of ad-hoc networks so that basic operations of systems including routing could be performed efficiently. However, these networks are sensitive to various kinds of assaults. Distributed Denial of Service attack (DDoS) is one of the various teething issues which highly overload the resources. The repercussion of such attack will be further effecting the routing, Quality of Service (QoS) and security that will further require optimization. In order to optimize security, network must ensure data confidentiality, data integrity, and availability of services. This research synopsis provides a comprehensive outline for selecting secured hybrid routing protocol among the existing reactive and hybrid protocols based on their comparison analysis under DDoS attack. Research work will primarily focus on developing more efficient hybrid and multipath secured routing protocol for ad-hoc networks. Progressive computational intelligence methodology will be used to enable an analysis of complex security issues for the proposed protocol. Network Simulator (NS2) and MATLAB simulation will be utilized for the validation of the proposed approach. This research work aims to optimize different routing

SHORT SYNOPSIS



Excluding matches
less than 14 words

| 7% | 5% | 4% | 2% |
|---|---|---|---|
| SIMILARITY INDEX | INTERNET SOURCES | PUBLICATIONS | STUDENT PAPERS |

| | | |
|---|---|---|
| 1 | dblp.semanticscholar.org | 2% |
| 2 | Jegan Govindasamy, Samundiswary Punniakody. "A comparative study of reactive, proactive and hybrid routing protocol in wireless sensor network under wormhole attack", Journal of Electrical Systems and Information [illegible] 2017 | 1% |
| 3 | Raenu Kolandaisamy, Rafidah Md Noor, Ismail Ahmedy, Iftikhar Ahmad, Muhammad Reza Z'aba, Muhammad Imran, Mohammed Alnuem. "A Multivariant Stream Analysis Approach to Detect and Mitigate DDoS Attacks in Vehicular Ad Hoc Networks", Wireless Communications and Mobile Computing, 2018 | 1% |
| | [illegible]ine.org | 1% |
| | [illegible] RK Univers[illegible] | |

<1%

<1%

7 Shishir Kumar, Prabhat Mahanti, Su-Jing Wang. "Intelligent computational techniques", Journal of Computational Science, 2018 <1%

8 link.springer.com <1%

9 shodhganga.inflibnet.ac.in <1%

Submitted to University of Huddersfield <1%

11 archive.org <1%

12 Danista Khan, Mahzaib Jamil. "Study of detecting and overcoming black hole attacks in MANET: A review", 2017 International Symposium on Wireless Systems and Networks (ISWSN), 2017 <1%

13 Yafang Wu, Shiwen Sun, Li Wang, Chengyi Xia. "Attack vulnerability of interdependent local-world networks: The effect of degree <1%

heterogeneity", IECON 2017 - 43rd Annual Conference of the IEEE Industrial Electronics Society, 2017

14 Security, Privacy, and Anonymity in Computation, Communication, and Storage", Springer Science and Business Media LLC, 2017 <1%